



最初にお読みください



AT-AR2050V/AT-AR3050S/AT-AR4050S リリースノート

この度は、AT-AR2050V/AT-AR3050S/AT-AR4050S をお買いあげいただき、誠にありがとうございます。このリリースノートは、取扱説明書とコマンドリファレンスの補足や、ご使用前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1 ファームウェアバージョン 5.4.5-2.3

2 本バージョンで追加・拡張された機能

ファームウェアバージョン 5.4.5-2.1 から 5.4.5-2.3 へのバージョンアップにおいて、以下の機能が追加・拡張されました。

2.1 ログ出力抑制機能

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「ログ」

ログ出力先ごとに、特定のログメッセージを出力させない設定が可能になりました。ログ出力の抑制は新しく追加された下記のコマンドで行います。

log exclude コマンド (グローバルコンフィグモード)

```
[no] log DESTINATION exclude {level LEVEL & facility FACILITY &  
program PROGRAM & msgtext TEXTLINE}
```

指定したログ出力先において、条件に一致したログメッセージを出力しないよう設定する。no 形式で実行した場合は、出力抑制の条件を削除する。

2.2 リミテッドローカルプロキシ ARP

 **参照**「コマンドリファレンス」 / 「IP ルーティング」 / 「ARP」

特定の IP アドレスに対してのみ ARP の代理応答を行うリミテッドローカルプロキシ ARP をサポートしました。

既存のローカルプロキシ ARP (ip local-proxy-arp コマンド) では、同一サブネット内のすべての IP アドレスに対して本製品が自身の MAC アドレスで代理応答しますが、リミテッドローカルプロキシ ARP では明示的に指定した IP アドレス範囲に対してのみ代理応答を行います。

リミテッドローカルプロキシ ARP の設定は、新しく追加された下記のコマンドで行います。

ip limited-local-proxy-arp コマンド (インターフェースモード)

```
[no] ip limited-local-proxy-arp
```

対象インターフェースでリミテッドローカルプロキシ ARP を有効化する。no 形式で実行した場合はリミテッドローカルプロキシ ARP を無効化する。初期設定は無効。

リミテッドローカルプロキシ ARP が有効なインターフェースでは、local-proxy-arp コマンド（グローバルコンフィグモード）で設定した範囲内の IP アドレスに対する ARP 要求にのみ、本製品が代理応答する。

local-proxy-arp コマンド（グローバルコンフィグモード）

```
[no] local-proxy-arp A.B.C.D/M
```

リミテッドローカルプロキシ ARP で代理応答する IP アドレス範囲を追加する。no 形式で実行した場合は指定した IP アドレス範囲をリミテッドローカルプロキシ ARP での代理応答対象から外す。

初期状態では未設定。

IP アドレス範囲は複数設定することができる。

3 本バージョンで修正された項目

ファームウェアバージョン 5.4.5-2.1 から 5.4.5-2.3 へのバージョンアップにおいて、以下の項目が修正されました。

- 3.1 フラッシュメモリーの空き容量がない状態で 5.4.5-1.x 以前から 5.4.5-2.1 にファームウェアを更新した場合、再起動後 CLI にログインできなくなりましたが、これを修正しました。なお、本修正にともない、フラッシュメモリーの空き容量がない状態で 5.4.5-1.x 以前から本バージョン以降に更新した場合は、権限レベル 1 ~ 14 のユーザーがすべて権限レベル 1 として扱われます。
- 3.2 AMF と EPSR の併用時、AMF マスターと AMF メンバー間のリンクタイプを、AMF クロスリンクから AMF リンクに変更した後は、AMF マスターと AMF メンバーそれぞれでリンクタイプ設定を保存して再起動する必要がありましたが、これを修正しました。

4 本バージョンでの制限事項

ファームウェアバージョン 5.4.5-2.3 には、以下の制限事項があります。

4.1 システム

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「システム」

検索ドメインリスト（ip domain-list）を設定する場合、最初にトップレベルドメインだけのものを設定すると、同一トップレベルドメインを持つ他のエントリーを使用しません。その結果、ホスト名を指定した Ping に失敗することがあります。

4.2 コマンドラインインターフェース

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「コマンドラインインターフェース」

- edit コマンドを使用すると、コンソールターミナルのサイズが自動で変更されてしまいます。
- enable コマンド（非特権 EXEC モード）のパスワード入力に連続して失敗した場合、エラーメッセージに続いて表示されるプロンプトの先頭に「enable-local 15」という不要な文字列が表示されます。
- do コマンド入力時、do の後にコマンド以外の文字や記号を入力しないでください。

4.3 ファイル操作

 参照「コマンドリファレンス」 / 「運用・管理」 / 「ファイル操作」

- Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB を装着している状態でシステムを再起動した場合、再起動時 SecureUSB メモリーの仕様によりロックがかかるため、再起動後に USB メモリーのセキュリティーを解除するための PIN コードを再度入力してください。
- edit, mkdir, rmdir, show file, show atmf backup コマンドを使用して Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB 上のファイルにアクセスした場合、ASK-256-8GB/16GB /32GB 上のアクセス LED が点滅状態のままになることがあります。その場合は、「dir usb:/」コマンドにて USB メモリーにアクセスする操作を行ってください。
- ファイル名にはスペースは使用できません。
- USB メモリーを装着した際、エラーメッセージが表示されることがありますが、これは表示だけの問題であり、動作に影響はありません。
- ECMP 経路を経由して行う TFTP でのファイル転送は未サポートです。
- フラッシュメモリーから SDHC カードまたは USB メモリーにファイルをコピーする時、途中で SDHC カードや USB メモリーを抜くと、実際はコピーに失敗しているにもかかわらず、(Fail を表すメッセージではなく、)「successful」というメッセージが表示されます。
- フラッシュメモリーから SDHC カードまたは USB メモリーにファイルをコピーする時、実際にコピーが完了しても、すぐにコピー完了のメッセージが表示されないことがあります。
- 起動用ファームウェアに設定されているフラッシュメモリー上のファイルと同名のファイルが外部メディア (USB メモリー、SDHC カード) に存在している場合、外部メディア上の該当ファイルを delete コマンドで削除できません。その場合は delete コマンドに force オプションを指定して削除してください。
- 機器に装着している USB メモリーまたは SD カードを抜き、再度機器に装着した時、以下のログが出ます。

抜いた時

```
kernel: FAT-fs (sda1): unable to read boot sector to mark fs as dirty
```

装着した時

```
kernel: FAT-fs (sda1): Volume was not properly unmounted. Some data may be corrupt. Please run fsck.
```

また、機器に装着している USB メモリーまたは SD カードを抜き、PC に装着すると、PC 上で「スキャンして修復しますか?」というメッセージが出ますが、ログのみの問題で、ファイルの破損はありません。

- move コマンドでファイルを移動する時、移動先と同じ名前のサブディレクトリーが存在する場合、移動に成功したというメッセージが表示されますが、実際には成功していません。その場合は、ファイル名を変更してから移動してください。

4.4 ユーザー認証

 **「コマンドリファレンス」 / 「運用・管理」 / 「ユーザー認証」**

- TACACS+ サーバーを利用したコマンドアカウントिंग (aaa accounting commands) 有効時、end コマンドのログは TACACS+ サーバーに送信されません。
- TACACS+ サーバーを利用した CLI ログインのアカウントिंगにおいて、SSH 経由でログインしたユーザーのログアウト時に Stop メッセージを送信しません。
- スクリプトで実行されたコマンドは TACACS+ サーバーへは送信されません。

4.5 RADIUS サーバー

 **「コマンドリファレンス」 / 「運用・管理」 / 「RADIUS サーバー」**

- server auth-port コマンドによりローカル RADIUS サーバーの認証用 UDP ポート番号を 63998 以上に設定しようとする時、関連プロセスが再起動するログが出力されます。また、上記の UDP ポート番号を使用してポート認証を行うことができません。
- ローカル RADIUS サーバーに登録するユーザー名の長さは 63 文字までにしてください。

4.6 ログ

 **「コマンドリファレンス」 / 「運用・管理」 / 「ログ」**

- no log buffered コマンドを入力してランタイムメモリー (RAM) へのログ出力を一度無効にした後、default log buffered コマンドを実行しても、ログ出力が再開しません。その場合は「log buffered」を実行することにより再開できます。
- permanent ログにメッセージフィルターを追加した後、default log コマンドを実行してログ出力設定を初期値に戻しても、追加したメッセージフィルターが削除されません。メッセージフィルターを削除するには、log(filter) コマンドを no 形式で実行してください。
- VLAN インターフェースで IPv6 マルチキャストパケットを受信した場合、以下の誤った MLD エラーログを出力しますが、通信に影響はありません。
kern.warning xxx kernel: Post MLD packet failed
kern.warning xxx kernel: Last message 'Post MLD packet fai' repeated 302 times, suppressed by syslog-ng on xxx

4.7 スクリプト

 **「コマンドリファレンス」 / 「運用・管理」 / 「スクリプト」**

- スクリプト機能を使って OSPF、BGP のルーティングプロセスを再起動することはできません。再起動が必要な場合はコマンドから直接実行してください。

- 間違ったコマンドを入力したスクリプトファイルを実行した場合、本来ならば、コンソール上に "% Invalid input detected at '^' marker." のエラーメッセージが出力されるべきですが、エラーメッセージが出力されないため、スクリプトファイルが正常に終了したかのように見えてしまいますが、通信には影響はありません。

4.8 トリガー

 **「コマンドリファレンス」 / 「運用・管理」 / 「トリガー」**

- トリガー設定時、script コマンドで指定したスクリプトファイルが存在しない場合、コンソールに出力されるメッセージ内のスクリプトファイルのパスが誤っています。

誤 : % Script /flash/script-3.scp does not exist. Please ensure it is created before
正 : % Script flash:/script-3.scp does not exist. Please ensure it is created before

また、スクリプトファイルが存在しないにもかかわらず上記コマンドは入力できてしまうため、コンフィグに反映され、show trigger コマンドのスクリプト情報にもこのスクリプトファイルが表示されます。

- 定時トリガー（type time）を連続で使用する場合は 1 分以上の間隔をあけてください。連続で実行すると show trigger counter で表示される Trigger activations のカウンターが正しくカウントされません。
- 複数のトリガーが同時に起動されると、「show trigger counter」で表示されるカウンターが正しい値を表示しなくなります。

4.9 SNMP

 **「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」**

- snmp-server enable trap コマンドにおいて、snmp-server の文字列を省略し、sn enable trap と入力すると、入力したコマンドがホスト名欄に表示され、コマンドは認識されません。コマンドは tab 補完などを利用して省略せずに入力してください。
- IP-MIB は未サポートです。
- VLAN 名を SNMP の dot1qVlanStaticName から設定する場合は、31 文字以内で設定してください。
- SNMP マネージャーから MIB 取得要求を連続的に受信すると、"ioctl 35123 returned -1" のようなログが出力されることがありますが、通信には影響ありません。

4.10 NTP

 **「コマンドリファレンス」 / 「運用・管理」 / 「NTP」**

- 初期設定時など、NTP を設定していない状態で show ntp status コマンドを入力すると、NTP サーバーと同期していることを示す以下のようなメッセージが表示されます。Clock is synchronized, stratum 0, actual frequency is 0.000PPM, precision is 2

- NTPv4 を使用している場合、ntp master コマンドによる NTP 階層レベル (Stratum) の設定と NTP サーバーによる時刻の取得を併用すると、NTP サーバーによって自動決定される階層レベルが優先されます。
- NTP による時刻の同期を設定している場合、時刻の手動変更は未サポートとなります。
- ntp master コマンドで <1-15> パラメーターを省略した場合、NTP 階層レベル (Stratum) は 6 になるべきですが、実際は 12 になります。この問題を回避するため、同コマンドでは NTP 階層レベルを明示的に指定してください。

4.11 仮想端末 (vty)

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「端末設定」

仮想端末ポート (Telnet/SSH クライアントが接続する仮想的な通信ポート) がすべて使用されているとき、write memory など一部のコマンドが実行できなくなります。

4.12 Telnet

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「Telnet」

- 本製品から他の機器に Telnet で接続しているとき、次のようなメッセージが表示されます。
No entry for terminal type "network";
using vt100 terminal settings.
- 非特権モードでホスト名を使用して、Telnet 経由でリモートデバイスにログインする場合は、ドメイン名まで指定してください。

4.13 Secure Shell

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「Secure Shell」

- SSH サーバーにおけるセッションタイムアウト (アイドル時タイムアウト) は、ssh server session-timeout コマンドで設定した値の 2 倍で動作します。
- 本製品の SSH サーバーに対して、次に示すような非対話式 SSH 接続 (コマンド実行) をしないでください。
※ 本製品の IP アドレスを 192.168.10.1 と仮定しています。
clientHost> ssh manager@192.168.10.1 "show system"
- SSH ログイン時、ログアウトするときに以下のログが表示されますが、動作に影響はありません。
sshd[2592]: error: Received disconnect from xxx.xxx.xxx.xxx: disconnected by server request
- manager 以外のユーザー名でログインする際、SSH 接続に RSA 公開鍵を使用した場合であってもパスワードが要求されますので、ユーザー名に紐づくパスワードを入力してください。
- AlliedWare 製品から AlliedWare Plus 製品への SSH 接続は未サポートです。

4.14 インターフェース

 **参照**「コマンドリファレンス」 / 「インターフェース」

- IPv6 アドレスを持つインターフェースに show interface コマンドを入力した際の結果に、実際のホップリミットの値が表示されません。
- LACP チャンネルグループがリンクダウンしているとき、show interface コマンドでは該当グループのパケットカウンターがすべて 0 と表示されます。

4.15 フローコントロール

 **参照**「コマンドリファレンス」 / 「インターフェース」 / 「スイッチポート」

show flowcontrol interface コマンドの RxPause カウンターが正しく表示されません。

4.16 ポートミラーリング

 **参照**「コマンドリファレンス」 / 「インターフェース」 / 「スイッチポート」

- 複数ポートにインターフェースモードのコマンドを発行するときは、interface コマンドで対象ポートを指定するときに、通常ポートとして使用できないミラーポートを含めないようにしてください。ミラーポートを含めた場合、一部のポートに設定が反映されなかったり、エラーメッセージが重複して表示されたりすることがあります。
- ミラーポートとして設定されたポートは、どの VLAN にも属していない状態となりますが、mirror interface none で、ポートのミラー設定を解除し VLAN に所属させても dot1qVlanStaticTable (1.3.6.1.2.1.17.7.1.4.3) にポート情報が当該 VLAN に表示されません。ポートに mirror interface コマンドでソースポートのインターフェースとトラフィックの向きを設定した後、設定を外すとポート情報が正しく表示されるようになります。

4.17 リンクアグリゲーション

 **参照**「コマンドリファレンス」 / 「インターフェース」 / 「リンクアグリゲーション」

- スタティックチャンネルグループ（手動設定のトランクグループ）において、shutdown コマンドによって無効にしていたポートに対して no shutdown コマンドを入力しても、ポートが有効にならないことがあります。この場合は、再度 shutdown コマンド、no shutdown コマンドを入力してください。
- スタティックチャンネルグループのインターフェースを shutdown コマンドにより無効に設定した後、リンクアップしているポートをそのスタティックチャンネルグループに追加すると、該当するインターフェースが再び有効になります。
- show interface コマンドで表示される poX インターフェース（LACP チャンネルグループ）の input packets 欄と output packets 欄の値には、リンクダウンしているメンバーポートの値が含まれません。LACP チャンネルグループ全体の正確な値を確認するには、poX インターフェースではなく各メンバーポートのカウンターを参照してください。
- トランクグループ（saX、poX）を無効化（shutdown）した状態でメンバーポートを削除しないでください。

- トランクグループ (saX、poX) のステータスを無効から有効に変更するときは、必ず saX、poX インターフェースに対して「no shutdown」を実行してください。メンバーポートに対して「no shutdown」を実行すると、該当ポートの所属するトランクグループに設定された機能が動作しなくなることがあります。誤ってメンバーポートに「no shutdown」を実行してしまった場合は、ケーブルを抜き差しすることで復旧します。
- リンクアグリゲーション (LACP およびスタティックチャンネルグループ) 使用時に show mac address-table コマンドを実行すると、チャンネルグループ番号ではなく実際に使用されているポート番号が表示されますが、これは表示だけの問題であり動作には影響ありません。

4.18 バーチャル LAN

 **「コマンドリファレンス」 / 「L2 スイッチング」 / 「バーチャル LAN」**

switchport trunk allowed vlan コマンドの except パラメーターに、該当ポートのネイティブ VLAN として設定されている VLAN を指定しないでください。except パラメーターでネイティブ VLAN を指定した場合、設定内容が正しくランニングコンフィグに反映されず、実際の VLAN 設定状態との間に不一致が発生します。

4.19 スパニングツリープロトコル

 **「コマンドリファレンス」 / 「L2 スイッチング」 / 「スパニングツリープロトコル」**

スパニングツリープロトコルにおいて、ポートの役割 (Role) が Rootport または Alternate から Designated に変更されると、ハロータイム × 3 秒後に下記のログが出力され、トポロジーの再構築が行われます。これによるトラフィックへの影響はありません。

```
BPDU Skew detected on port port1.0.1, beginning role reselection
```

4.20 ブリッジング

 **「コマンドリファレンス」 / 「ブリッジング」**

- 実インターフェースとその上に作成した 802.1Q サブインターフェースの Up/Down 状態が異なる場合、サブインターフェースに IP アドレスを設定することができません。サブインターフェースに IP アドレスを設定するときは、実インターフェースとサブインターフェースの Up/Down 状態を合わせてください。
- 複数の 802.1Q サブインターフェースに対して、同一の IPv4 アドレスや IPv6 アドレスを設定してもエラーになりませんのでご注意ください。
- L3 トンネルインターフェース (IPsec、GRE、IPv6) は 802.1Q サブインターフェースをサポートしません。これらのインターフェース上に encapsulation dot1q コマンドで 802.1Q サブインターフェースを作成してもエラーになりませんが、動作しないため設定しないでください。
- bridge-group コマンドでトンネルインターフェースをソフトウェアブリッジに割り当てるとき、次のようなメッセージが表示される場合がありますが、動作に影響はありません。

```
Warning: Interface tunnel0 is not fully configure yet
```

4.21 mtu コマンド

 **参照**「コマンドリファレンス」 / 「IP ルーティング」 / 「IP インターフェース」

VLAN インターフェース (vlanX) に対して mtu コマンドを実行すると、ランニングコンフィグ上では該当 VLAN のメンバーポートに対しても mtu コマンドを適用した状態になります。そのため、その状態で設定を保存すると、再起動時スイッチポートに対して mtu コマンドを実行できないためエラーメッセージが出力されますが、動作には影響ありません。

4.22 経路制御

 **参照**「コマンドリファレンス」 / 「IP ルーティング」 / 「経路制御」

- デフォルト経路を登録しているにもかかわらず、show ip route database コマンドで「Gateway of last resort is not set」と表示される場合がありますが、表示だけの問題で通信には影響ありません。
- IP 経路が 20 エントリー以上登録されていると、デフォルト経路を登録しているにもかかわらず、show ip route コマンドで「Gateway of last resort is not set」と表示される場合がありますが、表示だけの問題で通信には影響ありません。
- ネクストホップが直結サブネット上にないスタティック経路は未サポートです。
- show ip route コマンドで、デフォルトルート (0.0.0.0/0) にマッチするアドレスを指定した場合、経路が正しく表示されませんが、これは表示上の問題で実際の通信には問題ありません。
- 本製品が送出する ISAKMP メッセージはフローベース ECMP ではなく、パケットベース ECMP で送出されます。VPN 接続には影響ありません。

4.23 RIP

 **参照**「コマンドリファレンス」 / 「IP ルーティング」 / 「経路制御 (RIP)」

- RIP 認証機能において、複数のパスワード (キーチェーン) を設定した時、送信される RIP パケットの中に含まれるパスワードは、1 番目に設定したパスワードのみになります。
- RIP で通知するネットワークの範囲を指定するとき 32 ビットマスクで指定しないでください。
- cisco-metric-behavior コマンドは未サポートです。
- RIP パケットを送受信する RIP インターフェースの数は 250 までとしてください。

4.24 OSPF

 **参照**「コマンドリファレンス」 / 「IP ルーティング」 / 「経路制御 (OSPF)」

- OSPF において、代表ルーター (DR) として動作している時に clear ip ospf process コマンドを入力すると、隣接ルーターが DR に変更されます。
- OSPF の経路フィルタリングにおいて、match metric コマンドを使った特定経路の破棄ができません。

- OSPF で完全スタブエリア (area stub no-summary) に指定すると、本来そのエリア内にはデフォルトルートのみを通知するべきですが、各エリアへのルート情報 (タイプ 3LSA) が通知されてしまいます。
- 異なる OSPF プロセス間の OSPF 再通知は未サポートになります。
- overflow database コマンドを no 形式で実行した場合、設定を有効にするには再起動が必要となります。
- OSPF 環境でルートマップを使用して IP 経路表へ特定のネットワークのみの経路を登録させる場合、受信した LSU パケット内部の経路エントリーの最初から 255 個までしかルートマップの動作対象になりません。対向機器から受信するルート数は 255 以内におさまるようにしてください。
- OSPF モードおよび OSPFv3 モードの passive-interface コマンドで、インターフェースを指定せずに実行してすべてのインターフェースで有効にした後、no 形式で一部のインターフェースのみを無効にする操作は行わないでください。
- PPP インターフェース上に設定した IPsec トンネルインターフェースで OSPF を使用する場合は、該当 IPsec トンネルインターフェースに対して mtu コマンドを実行し、同インターフェースを通るパケットのサイズが 1300 バイト以下になるよう調整してください。
- OSPF を使用している環境でセカンダリー IP アドレスの設定を動的に行った場合、セカンダリー IP アドレスと同一サブネットのアドレス宛てに本製品の ssh コマンドや ping コマンドなどを実行した場合、始点アドレスとしてプライマリー IP アドレスをセットしたパケットを送信してしまいます。通信先でマネージメント ACL などのアクセス制限を行っている場合は、本製品のプライマリー IP アドレスからのアクセスも許可するよう設定してください。

4.25 BGP

参照「コマンドリファレンス」 / 「IP ルーティング」 / 「経路制御 (BGP)」

- BGP 経路の自動集約機能を有効に設定している場合、デフォルト経路 (0.0.0.0/0) のサブネットマスク長が 8 に変換されてしまいます。BGP の経路情報にデフォルト経路が含まれている場合は、自動集約機能を無効にしてください。
- ルートマップ上にある OSPF ルートは BGP 側に再配布されません。
- neighbor allowas-in コマンドを入力すると、BGP セッションが再起動され、通信が一瞬途切れることがあります。
- show ip bgp コマンドに「A.B.C.D/M」の形式でエントリーを指定して実行した時、iBGP ピアからプレフィックスの通知を受信しているにもかかわらず、ピアのルーター ID が 0.0.0.0 と表示されてしまいます。
- BGP の MD5 ダイジェスト認証使用時にパスワードを変更すると、Hold Time が満了するまでセッションを維持するため、新しいパスワードでセッションを張ることができません。

- IP 経路表に登録されているインターフェース経路は network synchronization コマンドを有効にしても BGP 経路表に追加されません。インターフェース経路を BGP 経路表に追加する場合は redistribute コマンドを使用してください。
- ルートリフレクターを設定している場合、ルートマップモードの set ip next-hop コマンドが正常に動作せず、ルートマップエントリにマッチした経路エントリのネクストホップアドレスを指定値に書き換えることができません。
- IPv6 BGP ピアの設定をする場合、固定 IPv6 アドレスを設定した VLAN インターフェースを指定してください。リンクローカルアドレスを使った場合は、Update メッセージに含まれる Nexthop に設定されたリンクローカルアドレスの値が正しく通知されません。
- IPv6 BGP において、neighbor default-originate コマンド (BGP IPv6 アドレスファミリーモード) でデフォルト経路を通知するよう設定している場合は、IPv6 BGP ピアとの通信にループバックインターフェースのアドレスを使うよう設定してください (本製品側では neighbor update-source コマンドで lo インターフェースを指定してください。また対向 BGP ピア側では本製品のループバックインターフェースのアドレスを接続先に指定してください)。
- IPv4 BGP において、neighbor default-originate コマンド (BGP モード) でデフォルト経路を通知するよう設定している場合は、ソフトウェアを実行しないでください。
- IPv6 の BGP 機能において、redistribute コマンドで static を指定するとデフォルトルートを BGP 経路表に追加してしまいます。
- iBGP セッションにおいて、ORIGINATOR_ID 属性値を「0.0.0.0」として通知してしまいます。
- IPv4/IPv6 BGP ピアとの接続状態が Established から Idle に変わった場合、show ip bgp summary、show bgp ipv6 summary コマンドの表示項目 Up/Down にはセッション切断後の経過時間が表示されるべきですが、Never と表示されます。
- IPv6 BGP で bgp nexthop-trigger enable コマンドを使用している場合、最適経路更新による通信復旧に時間がかかる場合があります。復旧時間を短縮したい場合は bgp scan-time コマンドで更新間隔を短くすることにより可能です。ただし、間隔を縮めすぎると CPU 使用率が高騰しやすくなるため、あらかじめご検証の上ご使用ください。
- show ip bgp コマンドで iBGP から学習した経路エントリを指定して詳細情報を表示した場合、Router-ID は 0.0.0.0 と表示され、正しい値を確認することができません。
- IPv6 BGP において、リカーシブルクックアップを利用して BGP 接続をする場合、IPv6 デフォルトルート経由での接続に失敗するため、IPv6 デフォルトルートを使用せずに宛先 IPv6 アドレスを指定してルートを設定してください。

4.26 ARP

「コマンドリファレンス」 / 「IP ルーティング」 / 「ARP」

- VRRP とプロキシ ARP の両方を有効にしている VLAN インターフェースにおいて、バーチャル IP アドレスがマスタールーターの実アドレスではない場合、接続機器からの ARP Request に対して、バーチャル MAC アドレスではなく受信インターフェースの実 MAC アドレスで応答することがあります。
- マルチキャスト MAC アドレスをもつスタティック ARP エントリーを作成した後、それを削除してから arp-mac-disparity コマンドを有効にして、同一のエントリーをダイナミックに再学習させる場合は、設定後にコンフィグを保存して再起動してください。
- 本製品の ARP Request に対して、ブロードキャストアドレス宛での ARP Reply が返ってきた場合、その情報は本製品の ARP キャッシュに登録されません。
- (AT-AR3050S/AT-AR4050S のみ) 片方の Ethernet インターフェースでリミテッドローカルプロキシ ARP (ip limited-local-proxy-arp コマンド) を有効にした場合、もう一方の Ethernet インターフェースでも同機能が有効になります。

4.27 VRRP

「コマンドリファレンス」 / 「IP ルーティング」 / 「VRRP」

- VRRP マスタールーターから自身の所有する IP アドレスでないバーチャル IPv6 アドレス宛てに Ping を実行できません。
- VRRP を使用していない装置では VRRP トラップを有効にしないでください。VRRP トラップの有効化・無効化は、snmp-server enable trap コマンドの vrrp オプションで行います。初期設定は無効です。
- VRRP のプリエンプトモードを有効にする場合は、バーチャルルーターの優先度が重複しないように設定してください。
- VLAN に IP アドレスを設定していない状態で VRRP の設定はしないでください。
- VRRPv3 を使用しているインターフェースの IPv6 グローバルユニキャストアドレスを変更する場合は、最初に当該インターフェース上のバーチャルルーターの設定を削除した後、IPv6 アドレスを変更し、その後バーチャルルーターの設定をしてください。
- ha associate コマンドを設定した状態でバーチャルルーターの設定を削除すると、HA LED が点灯したままになることがあります。バーチャルルーターの設定を削除する場合は、あらかじめ「no ha association」で HA モードの設定を削除した後、バーチャルルーターを削除してください。
- VRRP のステータス変更時に下記のログメッセージが出力されますが、VRRP の動作に影響はありません。

```
VRRPD[1255]: VRRP Event: Transition to MASTER state for 2/1/vlan[vid]  
HSL[1225]: HSL: ERROR: Insufficient space in Field Processor to add VRRP trap  
ARP entry
```

- VRRPv3 とローカルプロキシー ARP を併用時、実 IP を用いたマスタールーターではローカルプロキシー ARP は使用できますが、仮想 IP を用いたバックアップルーターではローカルプロキシー ARP が動作しません。
- IPv6 VRRP 機能を有効にしたインターフェースがダウンしても、show vrrp コマンドで表示される Multicast membership on IPv6 interface IFNAME のステータスが JOINED と表示されますが、表示上の問題だけであり VRRP の動作に影響はありません。

4.28 IPv6 ルーティング

 **「コマンドリファレンス」 / 「IPv6 ルーティング」**

- 自身の IPv6 アドレス宛に ping を実行するとエラーメッセージが表示されます。
- IPv6 において、VLAN が削除されたとき、リンクローカルアドレスが IPv6 転送表から消えません。
- フラグメントされた IPv6 Echo Request は利用できません。利用した場合 Duplicate パケットは正しく再構築されませんのでご注意ください。
- VLAN インターフェースに IPv6 アドレスを設定する場合、装置全体で 250 インターフェースを超えないようにしてください。
- 「no ipv6 forwarding」で IPv6 パケット転送機能を無効化した場合、下記の警告メッセージが表示されますが、実際には再起動は不要です。

% Warning: IPV6 forwarding will not be disabled until the switch reboots.
- IPv6 パケットに対しては ECMP が動作せず、1 つの経路だけを使用します。
- IPv6 アドレスに対して ping コマンドを実行してからすぐに Ctrl/C キーでキャンセルすると、コンソールがロックされる場合があります。IPv6 アドレスへの ping をキャンセルする場合は、ping 実行から 1 秒以上経過してからキャンセルしてください。なお、コンソールがロックされてしまった場合は、コンソールタイムアウト後に復旧します。

4.29 IPv6 インターフェース

 **「コマンドリファレンス」 / 「IPv6 ルーティング」 / 「IPv6 インターフェース」**

- 受信したルーター通知 (RA) パケットにより IPv6 インターフェースのアドレスを自動設定する場合、RA パケットに MTU オプションが設定されていてもその値を採用しません。
- DHCPv6 クライアント機能を使用した場合、DECLINE カウンターが動作しません。
- IPv4 アドレスと IPv6 アドレスの両方を設定している VLAN インターフェースで IPv4 の VRRP だけを有効にした場合、IPv6 Router Advertisement が送信されなくなります。

4.30 RIPng

 [「コマンドリファレンス」](#) / [「IPv6 ルーティング」](#) / [「経路制御 \(RIPng\)」](#)

cisco-metric-behavior コマンドは未サポートです。

4.31 OSPFv3

 [「コマンドリファレンス」](#) / [「IPv6 ルーティング」](#) / [「経路制御 \(OSPFv3\)」](#)

- OSPFv3 使用時、passive-interface コマンドで指定するパッシブインターフェースには、実在するインターフェースのみを指定してください。
- OSPFv3 の OSPF ネイバー暗号化方式を設定すると、次の不要なログが出力されます。これは表示だけの問題であり、動作には影響ありません。
Authentication/Encryption algorithm error, or SA key is wrong.
- OSPFv3 の AS 境界ルーターで集約された経路エントリが LSDB に登録されるときメトリックが 1 増加します。
- 経路集約により作成された null スタティック経路は IPv6 転送表 (FIB) に表示されませんので、show ipv6 route database コマンドで表示される IPv6 経路表 (RIB) で確認してください。
- OSPFv3 の認証機能は未サポートです。
- OSPFv3 で仮想リンクを使用している場合、グレースフルリスタートは未サポートです。
- IPv6 トンネルインターフェース上で OSPFv3 を使用しルート情報を交換した場合、対向のトンネルインターフェース上に割り当てられた IPv6 アドレスのみ 128 ビットマスクで登録されますが、通信に影響はありません。
- OSPFv3 において、自装置のトンネルインターフェースの経路情報を通知するとき、メトリックを 0 として通知します。
- エリア間経路として通知していたインターフェース経路を AS 外部経路に変更する場合は、最初に「no redistribute connected」を実行してから、「redistribute connected」を入力してください。

4.32 近隣探索

 [「コマンドリファレンス」](#) / [「IPv6 ルーティング」](#) / [「近隣探索」](#)

- イベントログ上に「Neighbor discovery has timed out on link eth1->5」のログメッセージが不要に表示されることがあります。これは表示上の問題であり通信には影響はありません。
- ipv6 nd reachable-time コマンドを使用することができません。Reachable Time フィールドは初期値のまま使用してください。

- (AT-AR4050Sのみ) ipv6 neighbor コマンドは未サポートです。
- (AT-AR2050V、AT-AR3050Sのみ) ipv6 neighbor コマンドでは Ethernet インターフェース上に Neighbor を登録できません。

4.33 PIM

参照「コマンドリファレンス」 / 「IP マルチキャスト」 / 「PIM」

- ip igmp static-group コマンドで登録したスイッチポートをタグなし、またはタグつきポートに変更すると、IGMP のエントリーは残っているにもかかわらず、PIM の (*,G) エントリーが削除された状態になります。
- PIM Prune メッセージを受信してもテーブル上から当該グループが完全に削除されないことがあります。ただし、マルチキャストパケットが転送され続けることはありません。(PIM-SMv4、PIM-SMv6 共通)

4.34 IGMP

参照「コマンドリファレンス」 / 「IP マルチキャスト」 / 「IGMP」

- show ip igmp groups コマンドの表示結果に、IGMP を有効に設定していない VLAN が表示されることがあります。これは show ip igmp groups コマンドの表示だけの問題であり、動作に影響はありません。
- IGMP プロキシにおいて、下流インターフェースに指定している VLAN を無効にしても、上流インターフェースにグループ情報が残り続けます。
- ip igmp proxy-service コマンドの設定を取り消す場合は、いったん対象 VLAN インターフェースを「shutdown」してから、「no ip igmp proxy-service」を実行し、その後 VLAN インターフェースを「no shutdown」してください。
- マルチキャストグループをスタティックに登録している状態で、同じマルチキャストグループをダイナミックに学習すると、その後スタティック登録したグループを削除しても、show ip igmp groups コマンドと show ip igmp snooping statistics interface コマンドの表示からは該当グループが削除されません。これは表示だけの問題で動作には影響ありません。
- clear ip mroute コマンドでマルチキャスト経路エントリーを削除すると、ip igmp static-group コマンドで設定した IGMP のスタティックエントリーも削除されてしまいます。clear ip mroute コマンド実行後は、ip igmp static-group コマンドを再実行してください。
- IGMP が有効化されている VLAN の所属ポートで受信した IGMP Leave メッセージは、同一 VLAN 内にフラッディングされます。
- IGMP プロキシ機能は、送信元指定付きの IGMPv3 パケットをサポートしていません。IGMP プロキシ使用時は、送信元を指定する機能のない IGMPv1、IGMPv2 か、送信元指定なしの IGMPv3 を使用してください。
- スイッチポートで受信した IGMP Query を他のスイッチポートに転送する時、IGMP エントリーを複製し 2 つ送信しますが、動作に影響はありません。

4.35 IGMP Snooping

 **「コマンドリファレンス」 / 「IP マルチキャスト」 / 「IGMP Snooping」**

- IGMP Snooping が有効な状態で、一旦無効にし、再度有効にした場合、その後受信する IGMP Report を全ポートにフラディングします。IGMP Snooping を再度有効にした後、clear ip igmp group コマンドを実行して全てのエントリを消去することで回避できます。
- Include リスト（送信元指定）付きのグループレコードが登録されている状態で、あるポートに接続された唯一のメンバーからグループ脱退要求を受信すると、そのポートには該当グループのマルチキャストトラフィックが転送されなくなりますが、他のポートで同じグループへの参加要求を受信すると、脱退要求によって転送のとまっていたポートでもマルチキャストの転送が再開されてしまいます（この転送は、脱退要求を受信したポートの Port Member list タイマーが満了するまで続きます）。
- ダイナミック登録されたルーターポートを改めてスタティックに設定した場合、ダイナミック登録されてから一定時間が経過すると設定が削除されます。また、一定時間が経過するまでの間、コンフィグ上にはスタティック設定が表示されますが、ip igmp snooping mrouter interface コマンドを no 形式で実行しても、コンフィグから削除することができません。
ルーターポートをスタティックに設定する場合は、該当のポートがダイナミック登録されていないことを確認してください。
- 未認識の IGMP メッセージタイプを持つ IGMP パケットは破棄されます。
- 不正な IP チェックサムを持つ IGMP Query を受信しても破棄しません。そのため、当該の IGMP Query を受信したインターフェースはルーターポートとして登録されています。
- IGMP Snooping 利用時、IGMP Querier を挟まないネットワーク上にマルチキャストサーバーとホストがいる場合、ホストが離脱した後もタイムアウトするまでパケットが転送され続けます。clear ip igmp コマンドで手動でエントリを削除してください。
- IGMP の Querier と IGMP Snooping が有効になっている機器が別に存在する場合、上位の Querier から Query を受け取った際に、レポート抑制機能によって自身がレポートを送信しますが、配下にグループメンバーが存在していない場合でも、Querier にレポートを送信してしまう場合があります。レポート抑制機能を無効化することで本現象は回避できます。

4.36 IPv6 マルチキャスト

 **「コマンドリファレンス」 / 「IPv6 マルチキャスト」**

- IPv6 環境でマルチキャストルーティングを使用する場合は、上流インターフェースで MLD Snooping を無効にしてください。
- IPv6 マルチキャスト機能において、OSPFv3 メッセージで使用するマルチキャスト MAC アドレスと同じ MAC アドレスを持つマルチキャストグループを使用している場合、shutdown コマンドで VLAN インターフェースを無効化 / 有効化すると、しばらくの間該当 VLAN に所属するポートでは OSPFv3 メッセージを破棄しますが、一定時間が経過すると自動的に復旧します。

4.37 PIMv6

参照「コマンドリファレンス」 / 「IPv6 マルチキャスト」 / 「PIM」

- PIMv6 使用時、PIMv6 インターフェースが最大まで設定されているとき、それらの VLAN の一つを削除しても、新たに VLAN インターフェースに PIMv6 を設定することができません。VLAN インターフェースから PIMv6 の設定を削除してから、VLAN を削除してください。
- VRRPv3 と PIM-SMv6 は併用できません。
- ipv6 pim ext-srcs-directly-connected コマンドは未サポートです。
- 本バージョンでサポートしている PIM-SMv6 は、ソース指定無しの JOIN (*,G)Join のみサポートで、ソース指定有りの JOIN (S,G)Join は未サポートとなります。
- 同一インターフェース上で ipv6 pim sparse-mode コマンドを繰り返し実行すると PIM-SMv6 が有効にならなくなる場合があるため、複数回実行しないでください。
- ipv6 pim spt-threshold コマンドを no 形式で実行しないでください。

4.38 MLD

参照「コマンドリファレンス」 / 「IPv6 マルチキャスト」 / 「MLD」

- MLDv2 において、グループエントリーがスタティック登録されている状態で、同じグループがダイナミックに登録され、待機時間が経過した時、ダイナミック登録されたエントリーとともに、スタティック登録されたエントリーもコンフィグから削除されます。
- clear ipv6 mld コマンド実行時に「% No such Group-Rec found」というエラーメッセージが表示されることがありますが、コマンドの動作には問題ありません。
- MLD パケットの Max Query Response Time フィールドの値が、本製品の設定の 1/100 の数値で送出されます。MLD をお使いの際は、ipv6 mld query-max-response-time コマンドでなるべく大きい値（最大値は 240）を設定してください。
- MLDv2 インターフェースにおいて、終点 IPv6 アドレスがマルチキャストアドレスの MLDv1 Report は受信しますが、終点 IPv6 アドレスが MLDv2 インターフェースのユニキャストアドレスになっている MLDv1 Report は受信せずに破棄します。
- MLD の Non-Queriers は、レコードタイプが BLOCK_OLD_SOURCES の MLDv2 Report メッセージを受信しても、指定された送信元アドレスを削除しません。
- MLDv1 と MLDv2 混在環境において、MLDv2 Report で Exclude モードになっている状態で、MLDv1 Report を受信した場合、該当アドレスは Exclude モードのソースリストから削除されているにもかかわらず、その後、該当アドレスからのマルチキャストパケットが転送されません。
- clear ipv6 mroute コマンドでマルチキャスト経路エントリーを削除すると、ipv6 mld static-group コマンドで設定した MLD のスタティックエントリーも削除されてしまい

ます。clear ipv6 mroute コマンド実行後は、ipv6 mld static-group コマンドを再実行してください。

- clear ipv6 mld group * ですべてのグループを削除した場合、ルーターポートのエントリも削除されてしまいます。
clear ipv6 mld group ff1e::1 のように特定のグループを指定した場合は削除されないため、グループを指定し削除してください。また、削除されてしまった場合も MLD Query を受信すれば再登録されます。
- スタティック MLD グループを設定した後、clear ipv6 mld コマンドでマルチキャストグループを指定すると、ランニングコンフィグからスタティック MLD グループが削除されます。
- ipv6 mld static-group コマンドを設定したポートにおいて、そのマルチキャストグループを持つ MLD Join メッセージを受信した状態で、shutdown コマンドによりポートをダウンさせた場合、ランニングコンフィグ上から ipv6 mld static-group コマンドを削除しますので、本コマンドを設定したポート上で shutdown コマンドを実行しないようにしてください。

4.39 MLD Snooping

 **「コマンドリファレンス」** / **「IPv6 マルチキャスト」** / **「MLD Snooping」**

- MLD Snooping の Report 抑制機能が有効なとき（初期設定は有効）、ルーターポートで受信した MLDv1 Report または Done メッセージを受信ポートから再送出してしまいます。これを回避するには、「no ipv6 mld snooping report-suppression」で Report 抑制機能を無効化してください。
- MLD Snooping を無効にしても一部の MLD Snooping の機能が動作し続けます。このため、show コマンド上の MLD エントリが更新されつづけたり、MLD のパケットを受信した際に MLD が動作していることを示すログが出力されます。

4.40 UTM

 **「コマンドリファレンス」** / **「UTM」**

- Web コントロールモードの rule コマンドを no 形式で実行するとき（ルールを削除するとき）、存在しないルール番号を指定してもエラーになりません。ルール番号をミスタイプした場合など、削除したつもりルールが削除されていなくても気付かない可能性があるため、ルール削除時にはご注意ください。
- ファイアウォールと NAT の最大ルール数は両機能あわせて 500 ですが、ルール数が 500 に近づくにつれてパフォーマンスが低下するため、なるべくルール数は少なく設定してください。

ルール数が多い場合は、以下の事象が発生します。

- ・ ルール数が 500 の場合、すべてのルールが有効になるまで約 2 分半かかります。
- ・ ルールを読み込んでいる間はすべてのパケットを破棄します。
- ・ ルールを読み込んでいる間に show nat rule コマンドを実行すると、有効になる前のルールは「*」付きで表示され、Hits カウンターには -1 が表示されます。また、すべてのルールが有効になってから、カウンターが正常に動作するまで 45 秒かかります。

- 無効な NAT ルールが存在する状態で show nat rule コマンドを実行すると、次のようなログが出力されます。
yyyy mm dd hh:mm:ss user.err awplus firewalld: NAT: Sending iptables -t nat -L PORT_FORWARDING_RULE_10 -v -x 2>&1 | grep DNAT | awk '{print \$1}' failed
- アプリケーションコントロール (DPI) 機能を有効にした場合、NAT ルールにおいてアプリケーション「ftp」が正しく動作しなくなります。これを回避するため、アプリケーションコントロール (DPI) 機能を使用する場合は、下記のようにして FTP 通信を表すカスタムアプリケーション「ftp」を定義してください。

```
awplus(config)# application ftp
awplus(config-application)# protocol tcp
awplus(config-application)# sport 1024 to 65535
awplus(config-application)# dport 21
```
- 複数のユーザーが同時にアプリケーション定義やエンティティ定義の設定を行うと、コマンドが競合し、意図しない設定になることがありますので、同時に設定を変更しないようにしてください。
- Ethernet インターフェース (eth1 ~ eth2) 上でスタティック NAT を使用する場合、NAT グローバルアドレスとして該当インターフェースと異なる IP アドレスを使用するときは、同インターフェースでローカルプロキシ ARP (ip local-proxy-arp コマンド) を有効にするか、NAT グローバルアドレスに対応するスタティック ARP エントリを対向装置に設定してください。

4.41 トラフィックシェーピング

 [「コマンドリファレンス」](#) / [「トラフィック制御」](#) / [「トラフィックシェーピング」](#)

- トラフィックシェーピングルールを設定していない状態で仮想帯域を設定し、その後トラフィックシェーピング機能を有効にした場合、show traffic-shaping interface コマンドの結果が正常に表示されません。これを回避するには、最初にトラフィックシェーピング機能を有効にしてください。
- トラフィックシェーピングルールの設定時に、未定義のアプリケーションを指定するとエラーメッセージが出力されます。トラフィックシェーピングルールを設定するときは、使用するアプリケーションをあらかじめ定義してから、ルールを設定してください。
- トラフィックシェーピング機能を有効にしているとき、次のようなログメッセージが出力されることがありますが、動作には影響ありません。
kernel: HTB: quantum of class 10001 is big. Consider r2q change

4.42 DNS リレー

 [「コマンドリファレンス」](#) / [「IP 付加機能」](#) / [「DNS リレー」](#)

DNS リレーと VRRP を併用した場合、VRRP のバーチャル IP アドレス宛てに転送された DNS パケットを DNS サーバーに転送することができません。クライアントには VRRP のバーチャル IP アドレスではなく、VRRP マスタールーターの LAN 側実 IP アドレスをプライマリー DNS サーバーアドレスに、また VRRP バックアップルーターの LAN 側実 IP アドレスをセカンダリー DNS サーバーアドレスとして設定してください。

4.43 DHCP サーバー

 **参照**「コマンドリファレンス」 / 「IP 付加機能」 / 「DHCP サーバー」

- 同じ DHCP クライアントから 2 回目の割り当て要求があった場合、割り当て中の IP アドレスは show ip dhcp binding コマンドの実行結果で表示される IP アドレス割り当て状況に残ったままになります。リースしているアドレスの使用期間が満了すると、当該の IP アドレスは割り当て状況一覧から消去されます。
- show ip dhcp binding コマンドで DHCP クライアントへの IP アドレス割り当て状況を確認するとき、いくつかの DHCP プールに関する情報が表示されないことがあります。
- DHCP プールが複数設定された環境で show ip dhcp binding コマンドを使用する際は、DHCP プール名やクライアントの IP を指定した状態で実行してください。
- 多数の DHCP プールを作成している環境において、ネットワークアドレス部に 10 か 100 の数字を含む IP アドレス（10.1.1.1/24、172.16.100.5/24 など）を払い出した場合、10 の部分が 2～9 になっている別のアドレス（10.1.1.1 に対して 2.1.1.1 や 9.1.1.1 など）、および、100 の部分が 11～99 になっている別の IP アドレス（172.16.100.5 に対して 172.16.11.5 や 172.16.99.5 など）のリース情報が消えることがあります。

4.44 DHCP リレー

 **参照**「コマンドリファレンス」 / 「IP 付加機能」 / 「DHCP リレー」

- show counter dhcp-relay コマンドのカウンターが正しく表示されません。
- DHCP リレー機能において転送可能な DHCP メッセージの最大長を設定した場合、その最大長より大きなパケットを受信してもパケットを正しく破棄せず、DHCP オプションの一部を削除して転送してしまうことがあります。

4.45 DHCPv6 サーバー

 **参照**「コマンドリファレンス」 / 「IP 付加機能」 / 「DHCPv6 サーバー」

- 複数の DHCPv6 プールを設定する際は、アドレス範囲やプレフィックスが異なる DHCPv6 プールに重複しないように設定してください。
- DHCPv6 サーバー機能において、動的に割り当てるアドレスの最終有効時間が infinite（無期限）の場合、IPv6 アドレスを配布しても、show コマンドに反映されません。
- DHCPv6 サーバー使用時、DHCPv6 サーバー配下のホストに、DHCP プール内の IPv6 アドレスを固定設定しないでください。
- DHCPv6 プールのサポートリミットは 200 個です。

4.46 トンネルインターフェース

 **参照**「コマンドリファレンス」 / 「VPN」 / 「トンネルインターフェース」

- 複数のトンネルインターフェースで同じ対向アドレス（tunnel destination）を設定した場合、2 つ目以降のトンネルインターフェースでは対向アドレスの設定削除ができません。2 つ目以降のトンネルインターフェースで対向アドレスを変更したい場合は、

tunnel destination コマンドを再実行して上書き設定するか、いったん該当トンネルインターフェースを削除したのち、再作成してください。

- GRE および IPv6 トンネルインターフェースの TTL を tunnel ttl コマンドで変更した場合は、設定を保存して再起動してください。変更後に再起動しないと、ルーティングが正常に行われなくなることがあります。
- トンネルインターフェースを削除した場合、下記の不要なログメッセージが出力されますが、動作への影響はありません。

```
BGP[1293]: Parse error for message Link Down ret=-1
PIM-SMv6[1262]: Parse error for message Link Down ret=-1
PIM-DM[1272]: Parse error for message Link Down ret=-1
PIM-SM[1290]: Parse error for message Link Down ret=-1
```

- トンネルインターフェースの下位インターフェース（親インターフェース）に対して「shutdown」 / 「no shutdown」を繰り返し実行しないでください。繰り返し実行すると、トンネル経由の通信が行えなくなることがあります。
- トンネルインターフェースの MTU を変更すると次のようなエラーメッセージがログに出力されますが、通信には影響ありません。
user.err XXXX HSL[1253]: HSL: ERROR: Error finding iif L2 interface info 11
user.err XXXX HSL[1253]: HSL: ERROR: Group(xxx.xxx.xxx.xxx) Source
- tunnel source コマンドでは「lo」から始まる無効なインターフェース名を設定することができますが、動作しないため該当インターフェースを指定しないようにしてください。

4.47 IPsec

 **「コマンドリファレンス」 / 「VPN」 / 「IPsec」**

- 多数の IPsec over IPv6 トンネルインターフェースが同時に VPN 接続を開始した場合、不正な ISAKMP メッセージを送信することがありますが、その後正常な ISAKMP メッセージを送信するため、VPN 接続には問題ありません。
- 対向機器との IPsec 接続が切断されても ISAKMP SA および IPsec SA が削除されないことがあります。対向機器から新しい IPsec セッションが開始されれば新しい SA を作成します。

4.48 L2TPv3

 **「コマンドリファレンス」 / 「VPN」 / 「L2TPv3」**

L2TPv3 トンネルインターフェース経由で SSH を使用する場合は、mtu コマンドで L2TPv3 トンネルインターフェースの MTU を 1300 バイト以下に設定してください。

4.49 OpenVPN

 **「コマンドリファレンス」 / 「VPN」 / 「OpenVPN」**

- OpenVPN Tun(L3) トンネルインターフェースの設定時、「IP packet with unknown IP version=15 seen」というログメッセージが出力されることがありますが、動作に影響はありません。
- OpenVPN トンネルインターフェースは同時に2つまで使用可能です (Tun モードと Tap モードを1つずつ)。なお、2つ同時に使用する場合は、各トンネルインターフェースで異なる UDP ポート番号を使用するように設定してください (tunnel openvpn port コマンド)。

4.50 GRE

 **「コマンドリファレンス」 / 「VPN」 / 「GRE」**

- IPsec 保護 (tunnel protection ipsec) を適用している GRE トンネルインターフェース上にトラフィックが存在する状態で該当インターフェースがダウンした場合、informational レベルの下記ログメッセージが繰り返し出力されます。ただし、本ログメッセージは informational レベルのため、初期設定では buffered ログ、permanent ログには保存されず、show log、show log permanent コマンドでも確認できません。

```
iked: [INTERNAL_ERR]: ikev2_auth.c:555:ikev2_auth_verify(): 4:xx.xx.xx.xx[500]  
- yy.yy.yy.yy[500]:(nil):no shared key with peer
```
- GRE トンネルインターフェースにおいて、MTU よりサイズの大きいパケットを受信した場合、本来なら ICMPv6 の「Packet Too Big」を返すべきですが、「Destination Host Unreachable」を返します。
- GRE トンネルインターフェースにおいて、対向装置までの経路 MTU が GRE トンネルインターフェースの MTU よりも小さい場合、本製品は LAN 側から受け取った IPv6 パケットを破棄し、送信元に ICMPv6 Packet Too Big エラーメッセージを返すべきですが、エラーを返送せずに IPv6 パケットを GRE パケットにカプセル化してトンネル対向に向けて送信します。
- GRE over IPv6 トンネルインターフェースの MTU 値をいったん設定した後で他の値に変更したときは、設定を保存してから再起動してください。

4.51 アライドテレシスマネージメントフレームワーク (AMF)

 **「コマンドリファレンス」 / 「アライドテレシスマネージメントフレームワーク」**

- AMF リンクとして使用しているスタティックチャンネルグループの設定や構成を変更する場合は、次に示す手順 A・B のいずれかにしたってください。

[手順 A]

1. 該当スタティックチャンネルグループに対して shutdown を実行する。
2. 設定や構成を変更する。
3. 該当スタティックチャンネルグループに対して no shutdown を実行する。

[手順 B]

1. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して `no switchport atmf-link` を実行する。
 2. 設定や構成を変更する。
 3. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して `switchport atmf-link` を実行する。
- リポートローリング機能でファームウェアバージョンを A から B に更新する場合、すでに対象ノードのフラッシュメモリー上にバージョン B のファームウェアイメージファイルが存在していると、ファームウェアの更新に失敗します。このような場合は、対象ノードから該当するファームウェアイメージファイルを削除してください。
 - AMF ネットワーク内にマスターノードが存在しない場合でも AMF ネットワークが構成できてしまいますが、AMF 機能は利用できません。
 - AMF マスターが AMF メンバーよりも後に AMF ネットワークに参加するとき、AMF マスターのコンフィグにてその他メンバーからのワーキングセット利用やリモートログインに制限がかけてあっても、既存のメンバーに対してこれらの制限が反映されません。再度 AMF マスター上で `atmf restricted-login` コマンドを実行することで、全ての AMF メンバーに対して制限をかけることができます。
 - `atmf backup bandwidth` コマンドのオンラインヘルプにおいて、AMF バックアップデータの転送に使用する帯域を `Okbps` に制限することができるようなヘルプメッセージが表示されます。実際には、値に `0` を指定した場合、`atmf backup bandwidth` コマンドを `no` 形式で実行したときと同様、AMF バックアップデータの転送に使用する帯域の制限が解除されます。
 - AMF マスター上で `atmf recover` コマンドによってメンバーノードの内蔵フラッシュメモリーの復元を実行した場合、復元が完了しても、マスターノード上で完了を示すメッセージが出力されません。復元の完了は、対象ノードにおけるログ出力によって確認できます。
 - ワーキングセットプロンプトでは `do` コマンドを使用できません。
 - オートリカバリーが成功したにもかかわらず、リカバリー後に正しく通信できない場合は、代替機の接続先が交換前と同じポートかどうかを確認してください。誤って交換前とは異なるポートに代替機を接続してしまった場合は、オートリカバリーが動作したとしても、交換前とネットワーク構成が異なるため、正しく通信できない可能性がありますのでご注意ください。
 - `atmf cleanup` コマンドの実行後、再起動時に HSL のエラーログが表示されますが、通信には影響はありません。
 - `no atmf enable` で AMF 機能を無効化しても、AMF 自動バックアップ機能が動作しようとし、バックアップファイルは保存されませんが、空のフォルダーが作成され、ログが出力されます。

- AMF ネットワーク名を変更すると、システム再起動を推奨するログの出力と共に、ノードの離脱、再加入が発生しますが、全ノードが再加入できないことがあります。AMF ネットワーク名を変更した後は、必ず再起動を行ってください。再加入できないノードに対しては、Telnetなどでログインし、再起動を実施してください。
- AMF マスターによる自動バックアップの実行時に本製品のバックアップが失敗することがありますが、次のバックアップタイミングでは成功します。
- バックアップ先 SSH サーバーに接続できない状況では、「show atmf backup server-status」コマンドの応答に 1 分程度の時間がかかります。
- HA モード VRRP を使用する AMF メンバーと、AMF マスターとの間で AMF 仮想リンクが 1 本のみ設定されている（VRRP マスタールーターとバックアップルーターの共通 IP アドレスを AMF 仮想リンクの終端アドレスとして指定した）構成において、VRRP マスタールーターがダウンした場合、他の AMF メンバーにワーキングセット経由で接続できなくなることがあります。このような構成で AMF 仮想リンクを使用する場合は、VRRP を構成する各 AMF メンバーの LAN 側 IP アドレスを終端アドレスとして、AMF 仮想リンクを複数設定してください。
- atmf working-set コマンドを no 形式で実行する場合は、グループ名を省略しないでください。
- AT-Vista Manager を使用時、DomainController/BackupDomainController になっている AMF メンバーの Management IPv6 Address がノード詳細画面に表示されません。
- ファームウェアバージョン 5.4.5-0.x 以前のファームウェアを使用している機器と、AMF 仮想リンクで接続した際に、AMF ネットワークへ正常に参加できないことがあります。接続するインターフェースの MTU 値を 1442 に変更することで正常に参加することができます。
- 同一デバイス間で複数のエリア仮想リンクを使用している時、一方の設定を削除した場合、リンクステータスは Active のままとなります。この時、もう一方のリンクのリンクステータスに Active と表示されるべきですが何も表示されません。これは表示上だけの問題であり通信に影響はありません。
- AMF マスターに挿入したローカルメディア（USB メモリー）の空き容量が足りない状態で AMF バックアップを実行した場合に出力するエラーメッセージが正しい宛先を示していませんが動作に影響はありません。
- LACP と AMF を併用している場合、LACP チャンネルグループのメンバーポートがリンクダウンすると、次のようなエラーログが出力されますが、これはログのみの問題で、AMF や通信には影響ありません。
kern.err XXXX kernel: Unexpected parent vlan4092 found for [IFNAME]
kern.err XXXX kernel: Parent interface vlan4092 found while deleting [IFNAME]
- HA モード VRRP を使用する AMF メンバーと、AMF マスターとの間で AMF 仮想リンクが 1 本のみ設定されている（VRRP マスタールーターとバックアップルーターの共通

IP アドレスを AMF 仮想リンクの終端アドレスとして指定した) 構成において、VRRP マスタールーターがダウンした場合、切り替え後の AMF メンバーで AMF のオートリカバリーができなくなることがあります。このような構成で AMF 仮想リンクを使用する場合は、VRRP を構成する各 AMF メンバーの LAN 側 IP アドレスを終端アドレスとして、AMF 仮想リンクを複数設定してください。

- shutdown コマンドがいずれかのインターフェースに設定されている AMF マスターをリカバリーすると以下のログが出力されますが、通信に影響はありません。
NSM[1091]: port1.0.31 enabling failed :-45
- AMF コントローラーとローカルマスターが別筐体で、かつ、同一エリアに存在する場合、ローカルマスターで `atmf restricted-login` コマンドを実行すると AT-Vista Manager のノードマップにおいて、同エリアの AMF ノードに対し SSH 接続ができません。
- AMF セーフコンフィグが適用されて AMF 接続ポート (AMF リンクまたは AMF クロスリンク) 以外のポートがすべてシャットダウンされる時、シャットダウンまでに数秒時間がかかることがあります。
- `atmf management subnet` コマンドでは、指定された IP アドレスに 16 ビットのサブネットマスク (255.255.0.0) を自動的に適用して AMF マネージメントサブネットの IP アドレス空間を決定しますが、同コマンドでクラス A の IP アドレスを指定した場合は、内部的に 8 ビットのマスクで経路を登録してしまいます。

たとえば、同コマンドで 10.0.0.0 を指定した場合、AMF マネージメントサブネットの範囲は 10.0.0.0/16 (10.0.0.0 ~ 10.0.255.255) ですが、これに対して 10.0.0.0/8 (10.0.0.0 ~ 10.255.255.255) を経路表に登録してしまいます。そのため、この範囲内のアドレス (たとえば 10.10.0.0/16) を運用ネットワーク (データプレーン) で使用していた場合、これらのアドレスを使用した通信ができなくなります。

これを回避するには、運用ネットワークで使用するアドレス範囲に対して、より具体的な (マスクの長い) 経路をスタティックに登録してください。たとえば、さきほどの例では、10.10.0.0/16 への経路を登録することで本現象を回避できます。

なお、本件は `atmf management subnet` コマンドでクラス A の IP アドレス (0.0.0.0 ~ 127.255.255.255) を指定したときにだけ発生する現象であり、クラス B、クラス C の IP アドレスを指定した場合は問題ありません。

5 マニュアルの補足

5.1 サポートする USB 型データ通信端末

サポートする USB 型データ通信端末につきましては、弊社ホームページでご確認ください。

5.2 サブスクリプションライセンス

 **「コマンドリファレンス」 / 「UTM」**

サブスクリプションライセンスはファームウェアバージョン **5.4.5-1.1** 以降でのみご使用いただけます。

5.3 サポートする OpenVPN クライアント

 **「コマンドリファレンス」 / 「VPN」 / 「OpenVPN」**

本バージョンでは、OpenVPN クライアントとして下記 OS/ アプリケーションの組み合わせをサポートします。

OS	アプリケーション
Windows7 (32bit)	OpenVPN GUI v5 (2.3.6)
	OpenVPN GUI v7 (2.3.7)
	OpenVPN GUI v7 (2.3.8)
	vpnux Client (ver.1.3.0.0)
Windows7 (64bit)	OpenVPN GUI v5 (2.3.6)
	OpenVPN GUI v7 (2.3.7)
	OpenVPN GUI v7 (2.3.8)
	vpnux Client (ver.1.3.0.0)
Windows8.1 (64bit)	OpenVPN GUI v5 (2.3.6)
	OpenVPN GUI v7 (2.3.7)
	OpenVPN GUI v7 (2.3.8)
	vpnux Client (ver.1.3.0.0)
Windows10 (64bit)	OpenVPN GUI v7 (2.3.8)
	vpnux Client (ver.1.3.0.0)
MAC OS X	Tunnelblick 3.4.3
	Tunnelblick 3.6 beta10
Android 4.4.x	OpenVPN for Android 0.6.29
	OpenVPN for Android 0.6.35
iOS 8	OpenVPN Connect 1.0.5

6 サポートリミット一覧

	AT-AR2050V	AT-AR3050S	AT-AR4050S
パフォーマンス			
VLAN 登録数	1000	4094	
MAC アドレス (FDB) 登録数	1024		
IPv4 ホスト (ARP) 登録数	1024		
IPv4 ルート			
IPv4 スタティックルート 登録数	1000		
RIPv1/v2 ルート 登録数	1500		
OSPFv2 ルート 登録数	1000		
BGP4 ルート 登録数	10000		
IPv6 ルート			
IPv6 スタティックルート 登録数	1000		
RIPng ルート 登録数	1500		
OSPFv3 ルート 登録数	1000		
BGP4+ ルート 登録数	10000		
リンクアグリゲーション			
グループ数 (筐体あたり)	2※1		
ポート数 (グループあたり)	4※2		
VPN			
IKEv1 同時接続可能セッション数	100※3	256※3	
IKEv2 同時接続可能セッション数	100※3	256※3	
L2TPv3 同時接続可能セッション数	256※3		
OpenVPN 同時接続可能セッション数	100※4		
PPPoE			
PPPoE 同時接続可能セッション数	20		
ローカル RADIUS サーバー ※5			
ユーザー 登録数	5000		
RADIUS クライアント (NAS) 登録数	1000		
ファイアウォール			
セッション数	65535		
ルール数	500※6		

※1 スタティックチャンネルグループと LACP チャンネルグループを合わせて 2 グループまでサポートします。

※2 LAN 側スイッチポートのみ使用可能です。

※3 共有するトンネルインターフェースの合計値です。

※4 vpnux Client (Windows 版) は 1 セッション、OpenVPN Connect (iOS 版) は 2 セッションまでをサポートします。

※5 OpenVPN でのみ使用可能です。

※6 ファイアウォールルールと NAT ルールを合わせて 500 ルールをサポートします。

7 最新マニュアルについて

最新の取扱説明書（613-002124 Rev.B）とコマンドリファレンス（613-002107 Rev.F）は弊社ホームページに掲載されています。

本リリースノートは、これらの最新マニュアルに対応した内容になっていますので、お手持ちのマニュアルが上記のものでない場合は、弊社ホームページで最新の情報をご覧ください。

<http://www.allied-tesesis.co.jp/>